



## California State Threat Assessment Center Bulletin

### *Critical Infrastructure and Key Resources*

PUB DATE: 2013-06-05

DOI: 20130417

STAC-20130605

#### The STAC Bulletin

provides comprehensive analyses of new, or updates of existing, intelligence issues.

#### WARNING:

The information marked UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE (U//LES) in this document is the property of the California State Threat Assessment Center (STAC) and may be distributed within the Federal Government (and its contractors), U.S. intelligence, law enforcement, public safety or protection officials and individuals with a need to know. Distribution beyond these entities without STAC authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the U//LES caveat may not be used in legal proceedings without first receiving authorization from the STAC.

## (U//FOUO) Attacks [REDACTED] in California's Communications Sector



### (U) ATTACK ON FIBER OPTIC LINES IN SAN JOSE [REDACTED]

(U//FOUO) [REDACTED]

[REDACTED] Unknown parties shot at and damaged a transformer at the Metcalf Road Pacific Gas and Electric<sup>USPER</sup> (PG&E) substation, then used hand tools to sever nearby fiber optic cables, disrupting local communications, including 911 services.



**Figure 1 – (U) Damaged transformer at Metcalf Substation**

Source: San Francisco Chronicle

(U//FOUO) [REDACTED]

[REDACTED] The substation and cables are located

#### (U) Source Summary and Confidence Level Statements

(U) We have high confidence in our judgments based on the nature of our sources, which were predominantly from reliable media outlets, telecommunications vendors, and official law enforcement reporting. Full information was not available on either incident due to the San Jose case being the subject of an ongoing investigation, and the lack of available first-hand reporting regarding the Egyptian case. However, our judgments are based on the basic nature of each attack, and we do not believe additional information would significantly alter our conclusions.

## UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

approximately one mile from the nearest residential neighborhood in a rural area located off a freeway, and neither asset had on-site security or staff present during the attacks. [REDACTED]

- (U//LES) On 18 April 2013, unknown actors breached a fence at the PG&E electrical substation located near Metcalf Road in San Jose. According to a Northern California Regional Intelligence Center (NCRIC) notification, the attackers breached the fence at the facility, and then used a rifle to shoot at and damage five transformers (see Figure 1).<sup>2</sup> Immediately prior to the attack, telecommunications personnel noticed a disruption in the Santa Clara County 911 system, which also disrupted AT&T<sup>USPER</sup> phone communications in the area. [REDACTED]



Figure 2 – Map location of PG&E substation damaged on 18 April 2013.

Source: Google



## UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

(U//FOUO) [REDACTED]

(U) An incident similar to the one in April 2013 occurred in April 2009 when unknown persons cut ten Verizon<sup>USPER</sup> underground cables at four locations in south San Jose. The outage affected emergency response networks, internet connections, phone services, and ATMs in Santa Clara, San Benito and Santa Cruz counties.

(U//FOUO) [REDACTED]

### (U) ATTEMPT TO SABOTAGE UNDERSEA FIBER-OPTIC CABLE IN EGYPT

[REDACTED]

(U//FOUO) [REDACTED]

- (U) On 27 March 2013, the Egyptian navy captured three as-yet unidentified men who were cutting the SMW-4 underwater fiber-optic cable at a cable landing in Alexandria.<sup>5</sup> According to pictures provided by naval officials, the men were equipped with SCUBA equipment and possibly hand tools for cutting the cable's insulation. The SMW-4 cable connects internet users in Europe, Africa, and Asia, stretching from France to Malaysia through the Mediterranean, the Arabian Sea, and the Indian Ocean.<sup>6</sup> The damaged cable caused a drop in internet speed in Egypt.<sup>7</sup> A map of the affected cable is below.

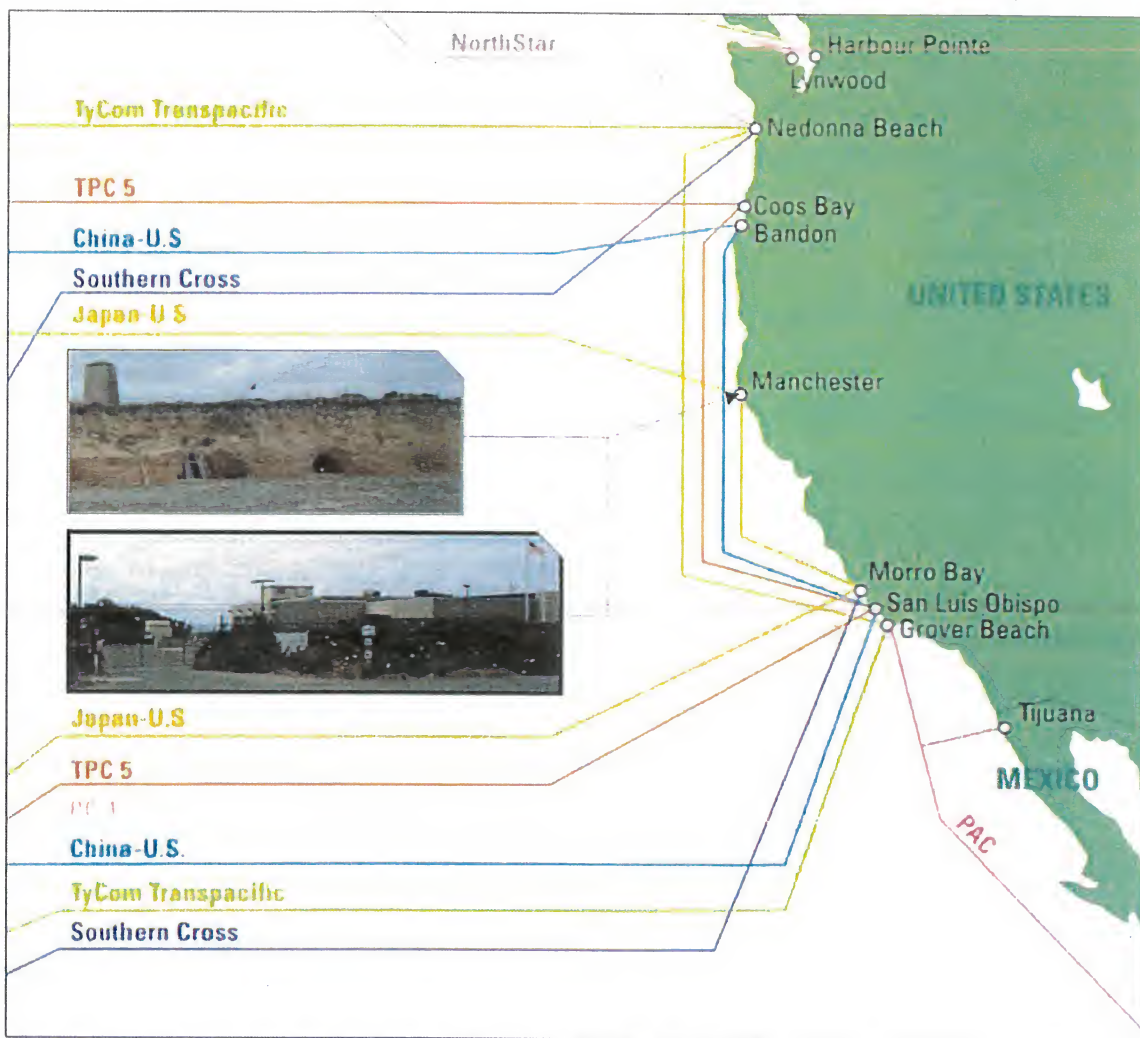
(U//FOUO) [REDACTED]

#### (U) Dry Plant

(U) According to DHS, a dry plant is a building co-located at a cable landing site containing electrical, switching, signal amplification, and routing equipment. Dry plants serve as a transfer point for intercontinental and domestic communications networks.

(U//FOUO) [REDACTED]

<sup>a</sup> (U) Cable landing stations contain operations equipment for powering up underwater repeaters and amplifiers. Cable termination stations, in contrast, are where cables physically connect to land-based networks.



**Figure 3 – (U) Map showing cable landing points in California.**

(U) There are 12 cable landing points in California with some sites co-located at the same facility. Note: The Monterey Bay Aquarium Research Institute<sup>USPER</sup> cable is not on this map, as it is a non-commercial scientific cable.<sup>9</sup>

(U) Inset: Cable entry sites and dry plant at Pont Arena Cable Station near Manchester, CA. Entry to the dry plant is restricted; however access to the beach is not. Dry plant access control measures include fencing, card readers, and security cameras.<sup>10</sup>

(U) Sources: TeleGeography and Telephone Central Offices



## UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

### (U) ADMINISTRATIVE NOTE

(U) For comments or questions related to the content or dissemination of this document, please contact the STAC at (916) 874-1100 or [STAC@calema.ca.gov](mailto:STAC@calema.ca.gov).

### (U) TRACKED BY

(U) HSEC-1.6.2.4, HSEC-7.6.2.4

### (U) FEEDBACK

(U) The STAC encourages your feedback using the survey found at <https://www.surveymonkey.com/s/VG5GZ2N>

### (U) ENDNOTES

<sup>1</sup> (U) Website; Vivek Alwayn; "Fiber-Optic Technologies"; posted 23 April 2004; <http://www.ciscopress.com/articles/article.asp?p=170740&seqNum=4>; accessed on 30 May 2013. Cisco is a U.S.-based telecommunications provider that designs, manufactures, and sells networking equipment.

<sup>2</sup> (U) Online Newspaper Article; No Author Listed; *CBS News*; "Vandalism At San Jose PG&E Substation Called 'Sabotage'"; 16 April 2013; <http://sanfrancisco.cbslocal.com/2013/04/16/gunshots-cause-oil-spill-at-san-jose-pge-substation/>; accessed on 23 April 2013.



<sup>4</sup> (U) Online Newspaper Article; Nanette Asimov, Ryan Kim, and Kevin Fagan; *San Francisco Chronicle*; "Sabotage Attacks Knock Out Phone Service"; 10 April 2009; <http://www.sfgate.com/bayarea/article/Sabotage-attacks-knock-out-phone-service-3245380.php>; accessed on 22 May 2013.

<sup>5</sup> (U) Online Newspaper Article; No Author Listed; *Associated Press*; "Egypt: Naval Forces Capture Three Divers Trying to Cut Undersea Internet Cable"; 27 March 2013; [http://www.washingtonpost.com/world/middle\\_east/egypt-naval-forces-capture-3-scuba-divers-trying-to-sabotage-undersea-internet-cable/2013/03/27/dd2975ec-9725-11e2-a976-7eb906f9ed9b\\_story.html](http://www.washingtonpost.com/world/middle_east/egypt-naval-forces-capture-3-scuba-divers-trying-to-sabotage-undersea-internet-cable/2013/03/27/dd2975ec-9725-11e2-a976-7eb906f9ed9b_story.html); accessed on 28 March 2013.

<sup>6</sup> (U) Internet Site; Telegeography; "Submarine Cable Map"; 26 March 2013; <http://www.submarinecablemap.com/>; accessed on 28 March 2013.

<sup>7</sup> (U) Online Newspaper Article; No Author Listed; BBC; "Egypt Arrests as Undersea Internet Cable Cut Off Alexandria"; 27 March 2013; <http://www.bbc.co.uk/news/world-middle-east-21963100>; accessed on 18 April 2013.



<sup>9</sup> (U) Website; TeleGeography; "2012 Submarine Cable Map"; 30 May 2013; <http://www.submarinecablemap.com/>; accessed on 30 May 2013. TeleGeography is a U.S.-based telecommunications market research and consulting firm.

## UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

---

<sup>10</sup> (U) Website; Telephone Central Offices; "Point Arena Cable Station"; posting date unknown; <http://www.thecentraloffice.com/Microwave/NMW/PARNCA/PARNCA01.htm>; accessed on 25 April 2013. Telephone Central Offices is a website operated by telecommunications equipment enthusiasts.



# CALIFORNIA STATE THREAT ASSESSMENT CENTER

## CRITICAL INFRASTRUCTURE PROTECTION (CIP) UNIT

### STANDALONE GRAPHIC – ENERGY SECTOR SNAPSHOT; ELECTRICITY SUBSECTOR

THE STANDALONE GRAPHIC PROVIDES A VISUAL ANALYSIS OF INTELLIGENCE ISSUES.

## (U) CIP Snapshot: Energy Sector; Electricity Subsector

(U//FOUO) [REDACTED] This product is intended for consideration by security and management personnel representing owners and operators of critical infrastructure systems in planning risk mitigation measures. The information cut off date on this product is 1 April 2017.

(U) CALIFORNIA SECTOR PROFILE	(U) THREAT SNAPSHOT	(U) PREPAREDNESS	(U) GAPS
<p>(U) The Energy Sector has three subsectors, electricity, oil, and natural gas. The electricity subsector provides the power that virtually all critical infrastructure sectors depend on for essential operations.</p> <p>(U) California (CA) is second in energy consumption behind Texas. Systemic and use efficiencies make it 49<sup>th</sup> out of 50 states in per capita consumption. CA leads the nation in solar power production and is third in wind.</p> <p>(U) CA's electricity subsector is comprised of 833 power plants and more than 15,000 miles of high tension lines. The rural nature of these assets make them difficult to protect.</p> <p>(U) The CA Energy Sector comprises 9 percent of CA's state significant infrastructure and includes approximately 114 assets that have been identified as meeting State significant criticality criteria.</p> <p>(U) Successful attacks or compromise by natural or technological hazards of the electricity subsector assets or the supply chains they depend on can result in denial of essential services or cascading effects that could severely impact the State's public safety and economic vitality.</p>	<p>Cyber Threats</p> <p>Technological Hazards</p> <p>Terrorism</p> <p>Natural Hazards</p>	<p>(U) CYBER</p> <p>(U) The Electricity Information Sharing and Analysis Center (EISAC)<sup>1</sup> acts as the threat information sharing entity in the Homeland Security Enterprise. ICS-CERT provides online training courses and cybersecurity tools at its website.<sup>2</sup> Integration of cyber-physical security at all phases of the planning and operating continuum is paramount.</p> <p>(U) TECHNOLOGICAL HAZARDS</p> <p>(U) Owner / operators should review EAPs, integrate mitigation planning, maintain their assets, and assess safety routinely. When possible, enhancing resiliency at the asset and system level should be considered by risk managers.</p> <p>(U) TERRORISM</p> <p>(U) Electricity subsector assets should periodically review their risk of a terrorism event. According to the California Office of Emergency Services 2015 Baseline Infrastructure Prioritization Report, 40 of the 114 assets meeting state criticality criteria in this sector have had on-site security assessments by DHS or OES from 2005 - 2015, including 18 of the 20 assets in the high risk category. The balance have used regional fusion center and private security assets for assessments. The best defense against terrorism is compliance with NERC CIP-14 standards and awareness and reporting of suspicious activity.<sup>3</sup></p> <p>(U) NATURAL HAZARDS</p> <p>(U) Owner / operators should review Emergency Action Plans (EAPs), integrate mitigation planning, and assess safety routinely. When possible, enhancing resiliency at the asset and system level should be considered by risk managers.</p>	<p>Further questions:  <a href="mailto:stac@caloes.ca.gov">stac@caloes.ca.gov</a></p>

1 March 2017  
 STAC-20170301  
<sup>1</sup> [www.eisac.com](http://www.eisac.com)  
<sup>2</sup> <https://ics-cert.us-cert.gov>  
<sup>3</sup> <https://calstas.org/>

CA 1: HSEC2 1: HSEC6.1  
 WARNING: This document was produced by the California State Threat Assessment Centers (STAC) Critical Infrastructure Protection Unit and is UNCLASSIFIED//FOR OFFICIAL USE ONLY. The primary audience for this is the critical infrastructure community, with an emphasis on critical infrastructure owners and operators – including privately and publicly owned critical infrastructure – and relevant information-sharing entities. It is meant for the widest distribution without the approval of an authorized STAC official.

UNCLASSIFIED//FOR OFFICIAL USE ONLY





## CALIFORNIA STATE THREAT ASSESSMENT CENTER

### NOTE – *CRITICAL INFRASTRUCTURE AND KEY RESOURCES*

THE STAC REFERENCE DOCUMENT IS AN INFORMATIONAL PRODUCT PROVIDING  
CLARIFICATION ON A PARTICULAR TOPIC, WITH NO COMMENT OR ANALYSIS.

PUB DATE: 201407DD  
DOI: 20140707  
STAC-201407XX

(U) Fiber Optic Lines Cut in San Jose, [REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

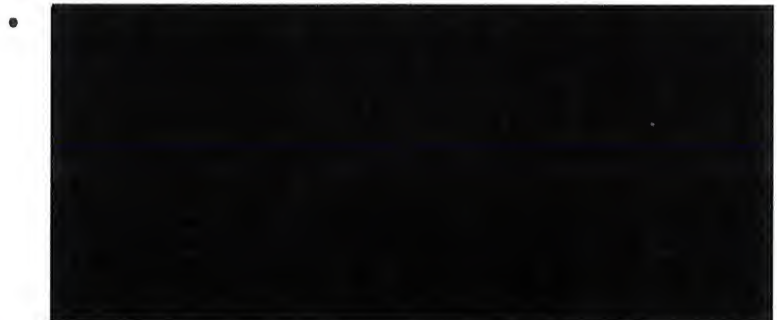
WARNING: This document is the exclusive property of the California State Threat Assessment Center (STAC) and is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the California Public Records Act (Govt. Code Sec. 6250-6720). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with STAC policy relating to U//FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need-to-know without prior approval of an authorized STAC official.





- (U//FOUO) SnowCrest<sup>USPER</sup>, an Internet provider in Siskiyou County, stated on their Facebook<sup>USPER</sup> page that their Internet and phone services were down on 7 July due to 3 fiber optic cables being cut "elsewhere in California".<sup>1</sup> The company's fiber backbone is CenturyLink, and this outage may be related the San Jose incident. Snowcrest also experienced an outage on 13 February due to a cut in a fiber-optic line between Sacramento and Yuba City.<sup>2</sup>

(U//FOUO) *There have been at least three similar incidents in California since 2011.*



- (U) On 14 June 2012, unidentified subjects cut two AT&T<sup>USPER</sup> underground fiber optic cables in Del Mar, CA. The attack led to an Internet cable television and landline phone service disruption across San Diego County. According to AT&T, the perpetrators had knowledge of the system and intended to disrupt service rather than steal equipment.<sup>5</sup>



Figure 4 – (U) Collapsed public safety communications tower near San Ramon, CA (SOURCE: KTVU<sup>USPER</sup>)



Figure 4 – (U) Repair of severed fiber optic lines in Del Mar, CA (SOURCE: NBC News)



Figure 4 – (U) Public safety communication sites in San Francisco, CA affected in July 2012 incident (SOURCE: Google<sup>USPER</sup> Maps)

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

- (U) On 9 April 2009, unknown parties severed ten fiber-optic communication lines in four underground vaults across San Jose, CA, disabling landline, cellular, and Internet service across Santa Clara, Santa Cruz, and San Benito Counties. Four lines in south San Jose were first cut, followed by two more at a location two miles away. Approximately two hours later, attackers cut four additional cables located in two locations in San Carlos.<sup>6</sup> According to local law enforcement officials, a special tool was required to open each vault, none of which were readily visible from the street.<sup>7</sup>

[REDACTED]

- (U//LES) On 16 April 2013, unknown actors damaged or destroyed multiple transformers at the Pacific Gas and Electric<sup>USPER</sup> electrical substation located near Metcalf Road in San Jose. According to a NCRIC notification, immediately prior to the attack, telecommunications personnel noticed a disruption in the Santa Clara County 911 system, which also disrupted AT&T phone communications in the area. [REDACTED]

[REDACTED]



UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

(U) ADMINISTRATIVE NOTE

(U) For comments or questions related to the content or dissemination of this document, please contact the STAC at (916) 874-1100 or [STAC@caloes.ca.gov](mailto:STAC@caloes.ca.gov).

(U) TRACKED BY

(U) HSEC-1.6.2.5

(U) FEEDBACK

(U) The STAC encourages your feedback using the survey found at <https://www.surveymonkey.com/s/XXXXXX>.

(U) ENDNOTES

<sup>1</sup> (U) Website; "SnowCrest Inc. – Mount Shasta, CA – Internet/Software | Facebook"; 7 July 2014; <https://www.facebook.com/pages/SnowCrest-Inc/178644392218862>; accessed on 8 July 2014.

<sup>2</sup> (U) Online Newspaper Article; No Author Listed; *Redding Record Searchlight*; "UPDATED: Snowcrest says Internet service is back"; 7 July 2014; <http://www.redding.com/news/local-news/cut-cables-interrupt-internet-provider-snowcrests-services>; accessed on 8 July 2014.

<sup>5</sup> (U) Online Newspaper Article; Tony Shin and Monica Garske; *NBC News*; "AT&T Cables Vandalized, \$250,000 Reward Offered for Information"; 15 June 2012; <http://www.nbcsandiego.com/news/local/ATT-Cables-Cut-Vandalized-250000-Reward-Offered-159155295.html>; accessed on 18 December 2013.

<sup>6</sup> (U) Online Newspaper Article; Nanette Asimov, Ryan Kim and Kevin Fagan; *San Francisco Chronicle*; "Sabotage attacks knock out phone service"; 10 April 2009; [http://articles.sfgate.com/2009-04-10/news/17191717\\_1\\_cables-debit-cards-vandals](http://articles.sfgate.com/2009-04-10/news/17191717_1_cables-debit-cards-vandals); accessed on 5 December 2011.

<sup>7</sup> (U) Online Newspaper Article; Lori Preuitt; *NBC News*; "\$250K Reward Out for Vandals Who Cut AT&T Lines"; 10 April 2009; <http://www.nbcbayarea.com/news/local/South-Bay-Dead-Zone.html>; accessed on 5 December 2011.

<sup>8</sup> (U) Online Newspaper Article; No Author Listed; *CBS News*; "Vandalism At San Jose PG&E Substation Called 'Sabotage'"; 16 April 2013; <http://sanfrancisco.cbslocal.com/2013/04/16/gunshots-cause-oil-spill-at-san-jose-pge-substation>; accessed on 14 July 2014.

<sup>10</sup> (U) Online Newspaper Article; Nanette Asimov, Ryan Kim, and Kevin Fagan; *San Francisco Chronicle*; "Sabotage Attacks Knock Out Phone Service"; 10 April 2009; <http://www.sfgate.com/bayarea/article/Sabotage-attacks-knock-out-phone-service-3245380.php>; accessed on 14 July 2014.

**Ducker, Tom@CalOES**

---

**From:** Nezhura, Lori@CalOES  
**Sent:** Monday, July 11, 2016 9:17 AM  
**To:** Ducker, Tom@CalOES; Wilson, Dena@CalOES  
**Cc:** Owen, Eli@CalOES; Lee, Doug@CalOES; [REDACTED]  
**Subject:** RE: RESPONSE REQUESTED: Information needed for Director's advanced brief

Hi Tom,

I am including Dena who is putting together the talking points for the Director, so she can follow-up with you regarding the information she needs.

Thanks much,

Lori

---

**From:** Ducker, Tom@CalOES  
**Sent:** Monday, July 11, 2016 7:53 AM  
**To:** Nezhura, Lori@CalOES  
**Cc:** Owen, Eli@CalOES; Lee, Doug@CalOES; [REDACTED]  
**Subject:** RE: RESPONSE REQUESTED: Information needed for Director's advanced brief

Lori,

There was no outage from Metcalf. Power was re-routed and additional generation capacity was brought online to stabilize the grid.

The new security guidelines are FERC/NERC CIP-14 standards.

Those standards set criteria for determining critical stations and required security plans/upgrades at those stations.

We have already screened the information we received from the California Energy Commission to see what stations are likely to fall under CIP-14 and we did an informal review of SoCal Edison's initial threat assessment that will be used for their CIP-14 review.

I can get you a summary of CIP-14, if you could use it.

I also have expanded information on Space Weather, EMP, etc., if you could use that.

Tom

---

**From:** Owen, Eli@CalOES  
**Sent:** Monday, July 11, 2016 7:41 AM  
**To:** Ducker, Tom@CalOES  
**Subject:** Fwd: RESPONSE REQUESTED: Information needed for Director's advanced brief

Plz field these . Cc me in response. Tx



Eli

Sent from my iPhone

Begin forwarded message:

**From:** "Wilson, Dena@CalOES" <[Dena.Wilson@CalOES.ca.gov](mailto:Dena.Wilson@CalOES.ca.gov)>  
**Date:** July 11, 2016 at 7:35:42 AM PDT  
**To:** "Owen, Eli@CalOES" <[Eli.Owen@CalOES.ca.gov](mailto:Eli.Owen@CalOES.ca.gov)>, "Nezhura, Lori@CalOES" <[Lori.Nezhura@CalOES.ca.gov](mailto:Lori.Nezhura@CalOES.ca.gov)>  
**Cc:** "Lee, Doug@CalOES" <[Doug.Lee@CalOES.ca.gov](mailto:Doug.Lee@CalOES.ca.gov)>, "Bout, Dan@CalOES" <[Dan.Bout@CalOES.ca.gov](mailto:Dan.Bout@CalOES.ca.gov)>  
**Subject:** RE: RESPONSE REQUESTED: Information needed for Director's advanced brief

Thank you Eli.

I have a couple of questions:

- The attack on the Metcalf Substation –
  - did it cause an outage? Notes indicated that a major outage was avoided. Was any outage experience before power was rerouted?
  - How many homes were effected?
  - How long did the outage last? [REDACTED]  
[REDACTED]. Please clarify.
  - What were the major revisions to security guidelines?

Thanks you in advance,  
Dena

---

**From:** Owen, Eli@CalOES  
**Sent:** Friday, July 08, 2016 5:52 PM  
**To:** Nezhura, Lori@CalOES  
**Cc:** Lee, Doug@CalOES; Wilson, Dena@CalOES; Bout, Dan@CalOES  
**Subject:** RE: RESPONSE REQUESTED: Information needed for Director's advanced brief

Draft attached. Will pick this up next week. Thanks.

---

**From:** Nezhura, Lori@CalOES  
**Sent:** Friday, July 08, 2016 3:55 PM  
**To:** Owen, Eli@CalOES  
**Cc:** Lee, Doug@CalOES; Wilson, Dena@CalOES; Bout, Dan@CalOES  
**Subject:** RE: RESPONSE REQUESTED: Information needed for Director's advanced brief

Happy Friday! Wondering if we can get what you have so far for the Director's EISS brief? Thanks!

---

**From:** Owen, Eli@CalOES  
**Sent:** Wednesday, July 06, 2016 4:58 PM  
**To:** Nezhura, Lori@CalOES; Wilson, Dena@CalOES; Bout, Dan@CalOES  
**Cc:** Lee, Doug@CalOES  
**Subject:** RE: RESPONSE REQUESTED: Information needed for Director's advanced brief

Copy Thanks.

---

**From:** Nezhura, Lori@CalOES  
**Sent:** Wednesday, July 06, 2016 4:51 PM  
**To:** Owen, Eli@CalOES; Wilson, Dena@CalOES; Bout, Dan@CalOES  
**Cc:** Lee, Doug@CalOES  
**Subject:** RE: RESPONSE REQUESTED: Information needed for Director's advanced brief

Correct. Because of the Director's busy travel schedule in the next two weeks, we need to get the AB to him sooner than expected. If this is a hardship for you, we can discuss.

---

**From:** Owen, Eli@CalOES  
**Sent:** Wednesday, July 06, 2016 4:46 PM  
**To:** Wilson, Dena@CalOES; Bout, Dan@CalOES  
**Cc:** Nezhura, Lori@CalOES; Lee, Doug@CalOES  
**Subject:** RE: RESPONSE REQUESTED: Information needed for Director's advanced brief

Sorry to be clear – the talk is 7/18 and you are requesting a response by 7/8?

---

**From:** Wilson, Dena@CalOES  
**Sent:** Wednesday, July 06, 2016 3:46 PM  
**To:** Owen, Eli@CalOES; Bout, Dan@CalOES  
**Cc:** Nezhura, Lori@CalOES  
**Subject:** RESPONSE REQUESTED: Information needed for Director's advanced brief  
**Importance:** High

**PLEASE RESPOND BY COB, Friday, July 8, 2016**

Eli/Dan,

The Director is participating in the Electric Infrastructure Security summit in London on July 18<sup>th</sup> to discuss planning, preparedness and response/recovery for "Black Sky" (*refers to the possibility of continental loss of the electrical grid that could be induced by a number of threats like nuclear electromagnetic pulse, cyber-attacks, severe space weather, etc.*) events surrounding Electrical Infrastructure Security and cybersecurity. In my discussion with the Director he was looking to cite some examples in California. He mentioned specifically the "Metcaf incident (sp?)". Could you provide me a summary of the incident and our response plus any other example similar to this? He would like to use a couple of examples for his remarks.

I would appreciate it. I have attached the summit agenda for convenience. Please let me know if you have any other questions.

Thank you in advance,  
Dena

*Dena Wilson*  
Office of Legislative and External Affairs  
California Governor's Office of Emergency Services  
3650 Schriever Avenue  
Mather, CA 95655  
Office: (916) 845-8940  
[www.CalOES.ca.gov](http://www.CalOES.ca.gov)





***Cal* OES**  
GOVERNOR'S OFFICE  
OF EMERGENCY SERVICES

## Ducker, Tom@CalOES

---

**From:** Ducker, Tom@CalOES  
**Sent:** Friday, October 28, 2016 8:47 AM  
**To:** Lyons, Doug@CHP (DLyons@chp.ca.gov)  
**Cc:** Lee, Doug@CalOES; Owen, Eli@CalOES  
**Subject:** FW: sample questions for SCE Full Scale Exercise

Here is my reply to a request for input on a possible question for next week's SCE round table.

Came in to my private email from Paul and resent on Cal OES email yesterday.

---

**From:** McGinnis, Paul@CalOES  
**Sent:** Thursday, October 27, 2016 11:41 AM  
**To:** Ducker, Tom@CalOES  
**Subject:** RE: sample questions for SCE Full Scale Exercise

Hi Tom,

I believe this response is indeed on target for the discussion that will be had at the SCE exercise roundtable. Thank you again for your assistance!

Best,

---

Paul McGinnis  
Legislative Analyst  
CA Governor's Office of Emergency Services  
Office Line: (916) 845-8105

---

**From:** Ducker, Tom@CalOES  
**Sent:** Thursday, October 27, 2016 11:24 AM  
**To:** McGinnis, Paul@CalOES  
**Subject:** RE: sample questions for SCE Full Scale Exercise

Paul,

Thanks. I take question five as referencing Wildfire impacts as stated in question one, but would suggest the answer focus on the regional, interconnect nature of the grid. Standards are set outside of Cal OES (Energy Commission/Public Utility Commission at the state or FERC/NERC at a higher level).

Here is a stab on some of the possible ways the regional nature of the grid could be addressed.

Question 5: How does this impact the ability to set new standards for infrastructure design?

First, this is a question that lies within both the California Energy Commission and Public Utility Commissions wheelhouses as they set guidelines and standards for private and public energy companies for the state.



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

As standards will need to be, at least, congruent (similar/consistent) across the states within the Region, close attention should be paid to standards proposed/adopted through the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC).

An example, in increasing physical security of sub-stations, is the Metcalf incident in California (shooter damaging transformers that lead to a shutdown) that sparked a renewed interest in security and the development of NERC's CIP-14.

More broadly, efforts to simplify and improve the use of response assets cross borders such as through EMAP (with Cal OES as an accredited agency) and the encouragement of solutions within the energy industry that improve information sharing and pooling of resources would help build upon a resilient design to make for effective and timely response.

---

Let me know if this is on target, or if we need something more technical for the Director on design standards.

Thanks again,

Tom

---

**From:** Tom Ducker [REDACTED]  
**Sent:** Thursday, October 27, 2016 8:11 AM  
**To:** Ducker, Tom@CalOES  
**Subject:** Fw: sample questions for SCE Full Scale Exercise

On Wednesday, October 26, 2016 10:50 AM, "McGinnis, Paul@CalOES" <[Paul.McGinnis@CalOES.ca.gov](mailto:Paul.McGinnis@CalOES.ca.gov)> wrote:

Hi all,

Below are a few questions that I received from SoCal Edison in advance of their full scale exercise taking place next week, Nov.2, 2016. I have put the name of the subject matter expert ID'd to best answer the questions that Dir. Ghilarducci may be asked during the Senior Leader's Roundtable discussion. If you could provide a brief answer where you see your name at your earliest convenience that would be

extremely helpful! If you believe someone else can provide further info or should answer any of the Q's please also let me know so I can reach out to them. I have also attached the agenda and exercise summary.

Thanks in advance for your assistance,

Paul McGinnis  
Legislative Analyst  
CA Governor's Office of Emergency Services  
Office Line: (916) 845-8105

---

**From:** Daniel Stevens [<mailto:Daniel.Stevens@sce.com>]  
**Sent:** Wednesday, October 26, 2016 8:42 AM  
**To:** McGinnis, Paul@CalOES  
**Subject:** sample questions

1. As evident in SCE's full scale exercise, severe wild fires can threaten the western interconnection [electric grid]. How would you prioritize competing response needs? **Don**
2. How does that impact the nuances of the public/private response coordination? **Abby**
3. How can emergency managers work with the private sector to prepare for, respond to, and recover from climate-related incidents? **Abby**
4. How will increasingly common and severe events impact emergency and risk management strategies? **Tina**
5. How does this impact the ability to set new standards for infrastructure design? **Tom**
6. How will state and local resource planning efforts for responding to and leading recovery efforts evolve with increased frequency and severity of climate related events? **Tina**
7. How will risk reduction programs inform planning efforts? **Tina**

Thanks,

Daniel Stevens, CEM  
Training & Exercise Program Manager  
Southern California Edison – Business Resiliency  
[Daniel.Stevens@sce.com](mailto:Daniel.Stevens@sce.com)  
626-302-6857 (o) / PAX 26857  
[REDACTED] (m)

Paul-  
Attached is the agenda for our external agency observers, which also includes a high level overview of the objectives. There are several areas we would like Mark to participate in during the day, which are very similar to his engagement last year during our Full Scale. Please let me know if you have additional questions.



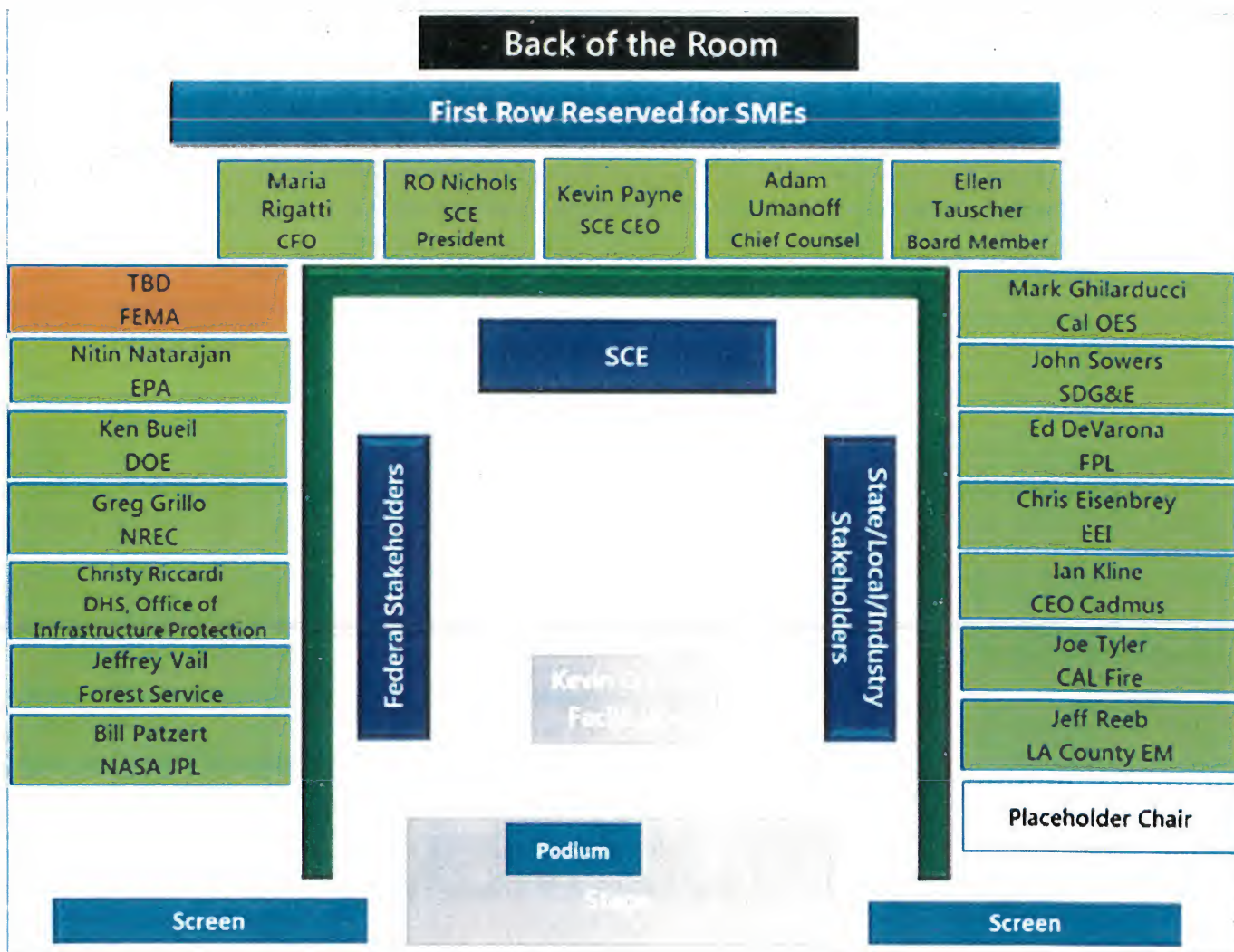
1. **Inject delivery.** Our company executives will be engaged in exercise play from about 8am until 10:30. We have 1 inject we would like Mark to call into the exercise, he just had to read from the script, which I included here:

Inject Time	From	To	Script
9:05 AM	Cal OES Director Mark Ghilarducci	CMC	Good Morning, this is Mark Ghilarducci, Director of Cal OES. I wa we are coordinating at all possible levels during this incident, partic across Southern California. I have asked my staff to coordinate with necessary. Are there any immediate resource needs or other asks of

2. **Mock-Press Brief.** Our CEO will be asked to give a press brief at 10:30 as part of the exercise. The purpose of the brief is to update the media/public on power outages and SCEs response to multiple wildfires impacting our infrastructure. Realistically it would be the county or a state press brief and not necessarily initiated by SCE. Similar to last year, we would like Mark to kick off the press-brief, essentially saying, we have called for this press brief so that SCE can provide an update on the outages. Mark will have a script (currently being developed) that he can read from, its just to kick off that part of the exercise. No real media will be present.

3. **Roundtable.** There will be about 23 external participants in a senior-level roundtable to discuss climate change and impacts to critical infrastructure. See participants below. Here are the objectives of the roundtable:

- a. Identify lines of responsibility for federal, state, local, and industry partners in mitigating and managing the effects of climate change on the national grid
- b. Explore key attributes of federal, state, local, and industry partners and identify potential opportunities for multi-partner response and resiliency planning
- c. Assess future state of climate resilience policy with respect to the electric utility industry
- d. Examine public and private approaches for identifying and overcoming financial and resource challenges related to mitigating and responding to multiple or simultaneous climate-related incidents impacting energy infrastructure



Thanks,

Daniel Stevens, CEM  
 Training & Exercise Program Manager  
 Southern California Edison – Business Resiliency  
[Daniel.Stevens@sce.com](mailto:Daniel.Stevens@sce.com)  
 626-302-6857 (o) / PAX 26857  
 (m)

**From:** McGinnis, Paul@CalOES [<mailto:Paul.McGinnis@CalOES.ca.gov>]  
**Sent:** Monday, October 24, 2016 2:03 PM  
**To:** Daniel Stevens <[Daniel.Stevens@sce.com](mailto:Daniel.Stevens@sce.com)>  
**Subject:** (External):SCE Full Scale Exercise Brief

Hi Daniel,

I am preparing an advanced brief for Cal OES Director Mark Ghilarducci with regards to the So Cal Edison Full Scale Exercise coming up on Wed. Nov 2. I have been notified he will be participating in both the mock press brief as well as the executive roundtable. I just had a few questions regarding the event that will assist me in drafting a brief for the Director



1. Will the Director be speaking at either the roundtable or the press brief, and if so are there any talking points to be made available?
2. Is there an agenda of events for the exercise?
3. Do you have an attendee list that you can share?
4. Any other information about the event that may be beneficial for Director Ghilarducci would be much appreciated

Thanks so much in advance of your review, and I look forward to hearing from you,

Best,

Paul McGinnis  
Legislative Analyst  
CA Governor's Office of Emergency Services  
Office Line: (916) 845-8105

**Ducker, Tom@CalOES**

---

**From:** Owen, Eli@CalOES  
**Sent:** Wednesday, February 14, 2018 11:41 AM  
**To:** Ducker, Tom@CalOES; Michael@CHP McCarthy  
**Cc:** [REDACTED]; [REDACTED]; Tresh, Keith@CalOES  
**Subject:** RE: MetCalf Incident 2013

This was very helpful – I called the WY HSA, on behalf of MG, and briefed the below. Thank you sir.

---

**From:** Ducker, Tom@CalOES  
**Sent:** Wednesday, February 14, 2018 7:01 AM  
**To:** Owen, Eli@CalOES; Michael@CHP McCarthy  
**Cc:** [REDACTED]; [REDACTED]; Tresh, Keith@CalOES  
**Subject:** RE: MetCalf Incident 2013

Eli,

It looks like this is a legislative related review. I'll get you a more detailed update by Friday. Bottom line is that federal regulation changed to increase security at sub-stations, our California legislature mandated a review of existing California regulation with a view to extending increased security to the distribution side of the grids, and utilities took additional security measures.

Tom

Tom Ducker, *CPP*  
Team Lead/IP Gateway Administrator/PCII Officer  
Critical Infrastructure Protection (CIP) Unit  
State Threat Assessment Center (STAC)  
California Governor's Office of Emergency Services  
[tom.ducker@caloes.ca.gov](mailto:tom.ducker@caloes.ca.gov)  
916-636-2917 (Desk)  
[REDACTED] (Cell)  
Certified Protection Professional (CPP®) - This certification designates individuals who have demonstrated competency in all areas constituting security management

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message. Thank you.

---

**From:** Owen, Eli@CalOES  
**Sent:** Tuesday, February 13, 2018 9:28 PM  
**To:** Ducker, Tom@CalOES; Michael@CHP McCarthy  
**Cc:** [REDACTED]; [REDACTED]; Tresh, Keith@CalOES  
**Subject:** Fwd: MetCalf Incident 2013

Fysa let me know if there is an update

By Friday if possible.

Sent from my iPhone

Begin forwarded message:

**From:** "Ghilarducci, Mark@CalOES" <[Mark.Ghilarducci@CalOES.ca.gov](mailto:Mark.Ghilarducci@CalOES.ca.gov)>  
**Date:** February 13, 2018 at 9:21:09 PM PST  
**To:** "Owen, Eli@CalOES" <[Eli.Owen@CalOES.ca.gov](mailto:Eli.Owen@CalOES.ca.gov)>, "Pal, Alex@CalOES" <[Alex.Pal@CalOES.ca.gov](mailto:Alex.Pal@CalOES.ca.gov)>  
**Cc:** "Pazin, Mark@CalOES" <[Mark.Pazin@CalOES.ca.gov](mailto:Mark.Pazin@CalOES.ca.gov)>  
**Subject:** Fwd: MetCalf Incident 2013

Eli, Alex, Mark

Please see email from Director Cameron in WYOMING. Is there an answer to his question?

M.

Begin forwarded message:

**From:** Guy Cameron <[guy.cameron@wyo.gov](mailto:guy.cameron@wyo.gov)>  
**Date:** February 7, 2018 at 10:54:47 AM PST  
**To:** "Ghilarducci, Mark@CalOES" <[Mark.Ghilarducci@caloes.ca.gov](mailto:Mark.Ghilarducci@caloes.ca.gov)>  
**Subject:** MetCalf Incident 2013

Good morning Mark,

I hope all is well. I wanted to ask if there has been any update on the MetCalf incident that occurred a few years back.

Mark, Wyoming's legislative session is kicking off next week and "Trespass Penalties" are being increased for those knowingly trespassing on Critical Infrastructure properties outlined in the bill. I understand there was an attempt to pass this legislation in Oklahoma this past year.

Thinking back to this California incident, thought it might be helpful to see if there were any action items that came of this event.

Thanks

Respectfully,

Guy

--

Guy Cameron  
Director  
Wyoming Office of Homeland Security  
[guy.cameron@wyo.gov](mailto:guy.cameron@wyo.gov)



(307) 777-8511

E-Mail to and from me, in connection with the transaction of public business, is subject to the Wyoming Public Records Act and may be disclosed to third parties.